Hybrid Blockchain-based environmentally friendly energy trading System

*** Partha Pratim Bhattacharjee [1], Chaitali Koley [2], Saibal Chatterjee [3]**
[1,2,3]National Institute of Technology, Mizoram, India
Email: [1]mat550.bu@gmail.com, [2]chaitali.ece@nitmz.ac.in, [3]saibalda@ieee.org

***Abstract* — This article presents a Hybrid Blockchain-based spotless and efficient clean and green power energy trading framework. A framework is recommended that gives a constant information-obtaining framework for exchanging and surveillance of the performance along with the health of these renewal energy-generating units. It can also provide a reasonable tariff plan for the trading of produced Power, of somewhat found spotless and environmentally friendly energy generating units. It typically works in a troublesome climate, and its security has forever been challenging. Node identification proof and authentication is a significant security worry for distributed IoT frameworks; blockchain technology with decentralization highlights another era of arrangements. Data/ Information is gathered and pre-processed utilizing the "Raspberry Pi 4 with 1 GB RAM Board" load-up alongside field sensors framing an "Edge Node (EN)", which comprises an inbuilt Wi-Fi unit, a generated terminal voltage sensor, load current sensors, an external real-time clock circuit, and other environmental surveillance sensor units for fundamental support of the generating unit. These IOT-based "Wireless Sensor Network (WSN)" nodes are separated into "Edge Node (EN)", "Fog Node (FN)", "Fog Node Base Station (FNBS)", and "Cloudlet Server (CS)", as indicated by their capacities and work conveyances which are framed into various network level. A private Blockchain is developed among the end nodes, which is an EN, subsequently, a public Blockchain is used for the next higher level of network nodes, which is the FN, hence it forms a complete hybrid blockchain-based wireless sensor network (HBWSN).**

Keywords* — *Hybrid blockchain, Ethereum blockchain, Edge Node, Fog Node, Fog Node Base Station, Identity Authentication.

I. INTRODUCTION

Global climate change and the development of environmentally friendly energy, drive the innovation of the distributed or decentralized power age. Appropriated power frameworks are viewed as a proficient, dependable, and eco-accommodating option in contrast to generally utilized non-renewable energy sources. The decentralized power framework is a limited-scale power-producing unit that coordinates with the electric conveyance framework, which is extremely close to the edge clients. As these are multi-source generating units and have clean and environmentally friendly power energy with zero Carbon discharge footprint, subsequently, they are turning out to be more well-known. Purchasers/ prosumers (a unit that can both consume and generate electric energy) can receive energy at less expense and achieve more financial goals through nearby influence age as well as connected load management, by utilizing microgrids or circulated energy frameworks [1].

The support and security of these dispersed units in an exceptionally distant territory is another test, and the development of qualified or prepared experts is unimaginable according to necessities. The subsequent test is deciding the power utilized from each disseminated producing unit by the associated nearby purchasers through the nearby microgrids.

IoT frameworks have an organization among sensors and nodes that go about as end clients, an organization between nodes of various layers, and intra-network participation between network nodes for offering different types of assistance. Subsequently, it is fundamental to deal with the character of sensor nodes which guarantees well-being as well as to understand the security authentication system between nodes. Since the climate sensor nodes placed in "Wireless Sensor Network (WSN)" are more complicated and vulnerable, it is vital to concentrate on the security validation between nodes in the WSN [2].

Blockchain-based IoT can make Pear to Pear (P2P) energy-exchanging stages more productive, so peers don't have to depend on incorporated centralized competent authority for their energy necessities [3]. Energy can be purchased from nearby energy showcases or generating units, which are produced from nearby sustainable power sources, although it is opposed by general utilities as it seems to receive from the primary power grid framework [4], [5]. Energy maintenance and surveillance stages utilizing IoT-based Blockchain can be more effective and controllable for users [6].

A few new approaches can be required when the domestic area embraces small and decentralized energy assets. The terrain where conventional grid power isn't accessible appropriately, that area can benefit from this new customary power market approach of electric power. This rising idea of prosumers currently needs a platform that can make surveillance entire of these environmentally friendly generating units. Customers and Prosumers can likewise screen out the trade of each other's energy needs straightforwardly.

The IoT security research concentrated fundamentally on two angles: the design of IoT-based WSN architecture and the superimpose of it [7]. This IoT security architecture for utilizing blockchain is primarily concentrated around the distributed qualities of IoT gadgets and how they fit in efficient mode with the blockchain geography, to accomplish the amalgamation of the legitimate construction of the blockchain can be more likely to serve the safety and security of the IoT devices. For verification and authentication, the current research for the most part constructs P2P networks utilizing

FNBSs, FNs, ENs, and different sensing units that can uphold the organization of the blockchain to shape a blockchain-based network and accomplish the identity authentication system of nodes in the WSN through the blockchain.

This article proposes a blockchain-based IoT network system, which has the accompanying commitments: It proposed a multi-WSN model with a few IoT nodes, and according to their capabilities they are classified as follows: FNBSs, FNs, ENs, for better administration and collaboration of IoT nodes applied in clean and green energy generating units. A hybrid blockchain model is represented here to be superimposed on the multiple WSN model-based green energy trading framework. In this framework, a private blockchain is proposed to be utilized between ENs, though a public blockchain is proposed to be utilized between FNs, to shape a hybrid blockchain. The progressive blockchain can have better execution.

II. **LITERATURE SURVEY**

A. It was introduced that, Sustainable power is the most emerging idea to tackle the power issue, particularly in distant villages [8]. Environmentally friendly power sources are financially savvy as well as profitable, for example, biogas, wind, sunlight-based (PVC), and hydroelectric power potential, due to the low running expense of generating units, which can be provided in remote spots. where the inventory of electric power from the grid is neither conceivable nor accessible [9].

B. One of the greatest difficulties in far-off regions without power is picking the appropriate mixing of feasible environmentally friendly clean and green energy arrangements. Already, one more work proposed Rules that can be utilized related to different materials and techniques to design a basic human empowerment project [10].

C. The execution qualities of IoT-based systems can be investigated according to a microarchitectural point of view, alongside the microarchitectural attributes that empower edge computing. To appropriately address a wide assortment of cutting-edge IoT applications inside the domain of the article, an expansive IoT application order procedure in light of use capabilities to empower speedier responsibility portrayals for IoT microcontrollers has been referenced. The article is a writing study (literature survey) alongside a conversation on microarchitectural enhancements as well as processing ideal models that empower the plan of the right-provisioned microcontrollers which are effective, configurable, versatile, and extendable [11].

D. A blockchain-based serverless decentralized IoT WSN architecture design was represented in this article for cultural applications, e.g., cloud producing, directed air or water quality examination, savvy rural financial aspects, energy-cognizant societal applications, and so on. These are planned to utilize a combination of very good quality figuring innovations, like Edge, Fog, and Cloud. It investigates the current IoT infrastructures and pinpoints the benefits of applying decentralized serverless blockchains to IoT designs [12].

E. "Blockchain-based Internet-of-Edge (BIoE)" is another innovation that consolidates IoT and endpoint registering frameworks with blockchain, which was proposed in the article. In addition to that, this article also proposed a versatile and controllable model for the IoT framework. It looks at the upsides of blockchain over edge computing for the foundation of a security safeguarding system while thinking about different limitations, for example, battery power, and so on. Here it was executed examination assessments running on the Ethereum blockchain [13].

F. The MQTT protocol used in "ESP8266" based "Mosquitto-based MQTT broker" system, to empower the residential apparatus surveillance and control mechanism, the same was introduced in this article [14].

G. This literature survey paper gives the subtleties of the vulnerable model relevant to the security of IoT-based WSN architectural systems. It likewise talks about the security prerequisites, different assaults, and attacks conceivable in an IoT-based WSN system environment. It likewise gave a basic writing literature review of ongoing interruption identification protocol for IoT and WSN conditions alongside their similar investigation. At long last, it talked about some challenges as well as research that can move and be taken care of in the future [15].

H. A multiple WSN security authentication system for IoT through blockchain, is proposed in this article. A blockchain-based system network is developed among different types of nodes for the formation of a "hybrid blockchain (HBC)" model, including nearby local public and private chains. The End node character confirmation activities are achieved by the nearby local blockchain, and group head node validation authentications are acknowledged in the public blockchain system [2].

I. This article proposed formal security check methods to countermeasure Threat models in validation authentication protocol for the IoT-based system. Likewise, scientific classification and correlation of verification and authentication protocol that is created for the IoT as far as the organization model, explicit security objectives, fundamental cycles, time complexity of computation, and communication between IoT nodes are explained [3].

III. **OBJECTIVE**

It is to find a total trading protocol as well as a P2P energy maintenance and surveillance system. This will determine the maintenance, well-being, surveillance, and usage of electric power generating units for consumers as well as prosumers, where quantities of generating units are more and set in extremely remote locations.

IV. **BRIEF OVERVIEW OF TECHNOLOGIES**

Here it will momentarily make sense of the innovative technology that can be utilized to configure as well as execute cycles of the proposed open-source P2P energy trade and exchange as well as the controlling mechanism. This P2P energy surveillance platform utilizes "hybrid blockchain (HBC)" through IoT-based WSN.

IV.I. **BLOCKCHAIN**

Initially, blockchain was introduced for P2P Bitcoin transaction systems. Each peer communicates as a miner,

bundles them in the middle among blocks, and adds them to a construction that resembles a chain-like data structure called a blockchain. A consensus protocol places each peer's blockchain as it is equivalent to the others. A blockchain is a database that is conveyed by every one of the Peers in a decentralized P2P network. Conversely, a blockchain can likewise be viewed as a P2P ledger record [16]. The accompanying significant ideas of blockchain are made sense of beneath:

Transaction: Something that occurs on the ledger is called a transaction, such as moving cash in a Ledger book. If one client has any desire to pay in cash (Bitcoin) to other clients, the cash (Bitcoin) proprietor is addressed by a singular code address, which is produced by the public key through the private key, and the proprietor signs electronically to the transaction. In the subsequent stage, the proprietor bundles the signature with other essential data (e.g., beneficiary, values, sensor data, and sensor information) into a data packet which is called a transaction. From that point forward, the data inside the exchange is broadcast to the organization of the network. It very well may be affirmed by each peer with the signature tag inside the data packet.

Block: To record the data of every one of the exchanges of the transactions that occurred in every period are utilized in Blocks. Each block of Blockchain comprises two sections: the substance part as well as the header part. The block header records the essential data like parent hash, hash, timestamp, Merkle-tree root, trouble, nonce, and so on. The block is a part of the blockchain containing the transaction numbers and the detailed payload of the transaction. The payload is the created information from different sensing units, e.g., sensor data, the same is valuable and essential for every node.

Chain: The gathering of several blocks connected along with one another is called a Chain, for instance, in Bitcoin, each block is distinguished by its hash value, which is a straightforward identification function. Each block produces after the past one to record the parent hash function of the past block. It tends to be looked at from the last block to the primary block, and it can be noticed the parent hash capability is in the block header. The chain-like construction resembles to be a rundown, as displayed in **Figure – 1**.

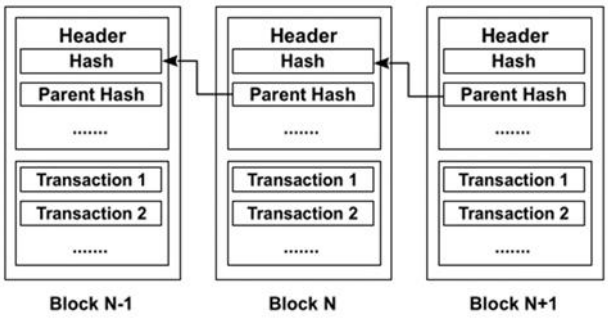

Figure – 1: The chain-like structure of Blockchain

Consensus: A “peer-to-peer protocol”, which is run by peers and mines is a Consensus protocol, the same is used for maintenance of the security and upkeep of the blockchain, nonetheless, each peer may not get a similar request of transaction due to the high organization idleness and requires a convention to conclude how transactions ought to be requested, for instance, Bitcoin uses “Proof of Work (PoW)” and Fabric uses “Practical Byzantine Fault Tolerance (PBFT)” algorithms, the same is expressed as the consensus protocol. It is proposed in this article that, this control arrangement can be utilized as “Proof of Work (PoW)” as a consensus protocol in “Ethereum Blockchain” of Private Blockchain among the ENs.

IV.II. BLOCKCHAIN-BASED NODE MANAGEMENT, SURVEILLANCE, AUTHENTICATION, AND VALIDATION SYSTEM

At present a new and emerging research topic is the Verification and Authentication of IoT Nodes in a blockchain-based framework. In [7], Hammi et al. recommended a decentralized blockchain-based gadget node for authentication and validation mechanisms for cloud-based nodes. In this proposed article "Edge Nodes" and "Fog Nodes" are put in an extremely far-off place where this technique is reasonably challenging, aside from that it doesn't uphold cross-domain correspondence. IoT Chain, a security design of the WSN based on IoT, which comprises a blockchain layer, application layer, and authentication, is proposed. Z. Bao et al. proposed an architecture where the expansion of a blockchain layer considers the conveyance of blockchain administrations on the IoT and the obtaining of transaction information from the application layer. Identifier validation and authentication, access control, security assurance, lightweight elements, territorial node adaptation to internal failure, denial of service elasticity, and storage capacity respectability are undeniably acknowledged by this engineering, as per security

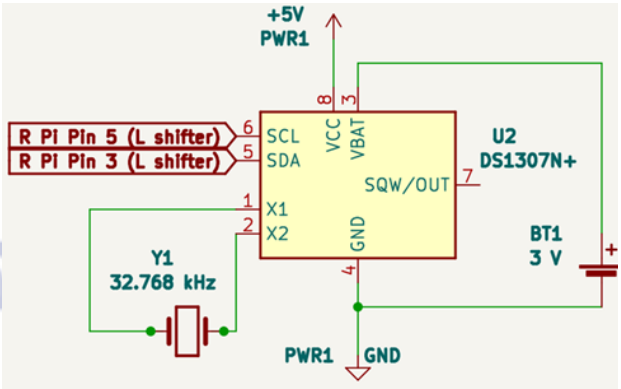

Figure – 2: The Real-Time Clock Circuit

investigation. In any case, this engineering partially ignores the constraints of most gadgets on the IoT giving a dispersed security construction to the IoT by utilizing the decentralized qualities of blockchain, regardless purposes of the concentrated validation authentication unit [17].

V. METHODOLOGY

V.I. EDGE NODES (EN)

In [18] Bhattacharjee, PP et al. recommended the Edge Node, which is straightforwardly associated with clean and green or environmentally friendly energy generating stations. EN is a blend of all essential equipment and hardware arrangements consisting of current sensing units, a voltage sensing unit, a "Real-time clock (RTC)" hardware (**Figure – 2**), a "Raspberry Pi 4 with 1 GB RAM" microcontroller board along with built-in Wi-Fi unit. It is additionally associated with other fundamental environmental observing and monitoring sensors along with security and controlling Relays. This little Board can run with an open-source embedded Linux OS. The same can be downloaded from the "Raspberry Pi" site and

installed as well. In our framework, we have utilized a 64-bit "Raspberry Pi" operating system, which is a "Debian Linux OS". This Board is straightforwardly interfaced with this environmentally friendly generating unit. At long last, it shapes the "Edge Node (EN)". It may be assumed that the output Voltage of every unit is 24V (rms) and it can be rectified through the Bridge rectifier. The Current sensing unit can measure the consuming current and producing current for the consumer and prosumer respectively. Another separate current sensing unit can be connected to measure prosumers' consumption.

In the Sensor segment, it has to be utilized: An RTC assembled by using a "DS1307" chip with a built-in I2C Bus interface, which is fundamental for the Blockchain time stamp, and the same circuit is displayed in **Figure – 2**. There are two I2C buses available in GPIO of the "Raspberry Pi" Board. Out of them, one can be connected for RTC, and the same is in Pin "3" and Pin "5" of GPIO. Practically speaking, it tends to be found, that "68H" is the location of the RTC through the I2C interface. It tends to be noticed that every one of the sensors connected with ADC, even RTC, and so on, are working with a 5 V supply, although "Pi" GPIOs' working voltage is 3.3 V, and this GPIO can supply 3.3 V (pin "1") and 5 V (pin "2" and "4") respectively. A "Bidirectional Logic Level Shifter" circuit is required for working with these peripherals, and the same is displayed in, **Figure – 3**. It tends to be expected that the no-load voltage of a 24V alternator (also PVC) unit can be raised to 54V as a safe side. The Voltage Sensing unit consists of two MFRs of 100kΩ and 10kΩ, connected in series across the alternator output, as a potential divider. It can be noted that Pi Boards have no inbuilt ADC, hence, a 16-bit four-channel ADC "ADS1115" can be utilized, that can work in the I2C Bus of GPIO as well. The detected voltage can be taken from this potential divider and across the 10kΩ resistor, to one channel (say "A0") of "ADS1115". The voltage detected values can fluctuate between "+32767" to "- 32768" absolute values. The ADC works with a 5 V supply.

Current Sensors can be utilized for detecting the producing/ consumed current of generating units. The Hall effect current sensor "ACS712" can be utilized for this purpose, it can detect the typical average value of DC and the rms value of AC. It is isolated from the source and detecting unit. The upper limit of the current sensing unit is 30 amps. In this manner, it tends to be presumed that the limit of the units is 720VA. The next free channel (say "A1") of "ADS1115" can be used for sensing the analog value of consuming current for prosumers as well as consumers. It is also required to detect the producing current of prosumers, the same can be sensed through the next free channel (say "A2"). Practically it is found that the "48H" (**Figure – 4**) location of the I2C bus is allotted for "ADS1115", as its 'ADDR' pin is grounded.

One of the Environmental sensing modules is the "DHT11", a "Temperature and Humidity Sensor Module" that can be utilized to detect ambient temperature along with atmospheric moisture. "DHT11" can give digital data, which is equivalent to ambient temperature and humidity. Any spare GPIO port, (say pin "11") of the "Pi" Board can be utilized for this purpose.

The Turbidity Sensor can be selected as the second Environmental sensor, which is "SKU 62828". It can be connected with the fourth channel ADC "ADS1115" (say "A3"). It very well may be noticed that the Turbidity increments, sensor output analog voltage diminishes. A regular module is 2.5V for "3000 turbidities" and 3.9V for "1000 turbidities" of a 5V inventory supply voltage. This sensor can be utilized for the Pico Hydel Power Plant. The "GUVA-S12SD UV" Sensor is reasonable for sensing ultraviolet (UV) radiation in daylight. It very well may be utilized for Sun oriented Power (Solar PVC), where it tends to be observed for how much UV light. This sensor can be utilized for the Solar Power system. This sensor can be interfaced with the same ADC "ADS1115" (say "A3"), as referenced previously.

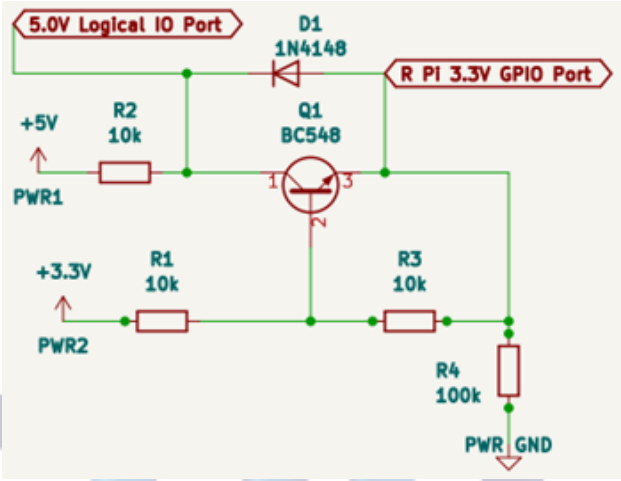

Figure – 3: The Connected I2C device addresses

Two I2C bus devices have been associated with EN, one for 4-channel ADC and another for RTC. Four ADC ports have been utilized: one for voltage, two for current, and a fourth one for turbidity/ UV detection. It can detect terminal voltage (average value) and rms value of generated current by prosumers along with consumed current by the consumers and prosumers. Surrounding Temperature and humidity sensors

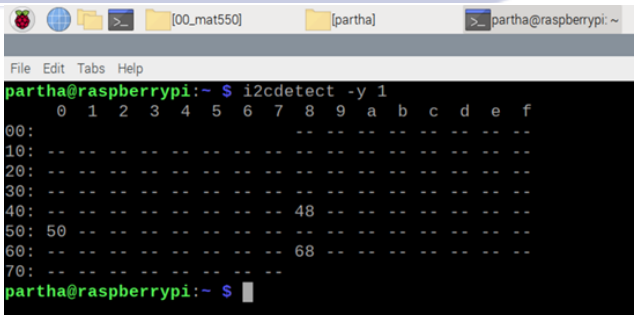

Figure – 4: The Connected I2C device addresses

can likewise be associated with one GPIO IN port (say pin "11"). Two GPIO OUT ports are utilized for prosumers (likewise consumers), which is for associating to connect the safety Relay/ Contactor. These Relay/ Contactor can be guaranteed for load adjusting between the Miniature Matrix for the local Microgrid and prosumers' self-requirements like their own homegrown lighting load or associated Battery charging load and so on. Nonconventional energy sources, such as Pico Hydel Power/ Solar Power/ Wind Power, can't create power at a similar rate for a whole day. It can disengage the connected load while generating unit yield voltage underneath the threshold limit. There must be one minute deferring between the activity pattern of the switch-off of the

relay/ contactor, in any case, relay chatting may happen. Hence, the safety of generating units is obtained. Each EN is wireless (Wi-Fi) linked with a FN as a client.

V.II. **FOG NODES (FN)**

A "Raspberry Pi 4 with 4GB RAM" microcontroller board can be used as a Fog Node (FN), which has slightly better performance than the Edge Nodes (ENs). This little Board can run with an open-source embedded Linux OS. The same can be downloaded from the "Raspberry Pi" site and installed as well. In our framework, we have utilized a 64-bit "Raspberry Pi" operating system (OS), which is a "Debian Linux OS", which was referenced before in EN. It has an underlying built-in Wi-Fi port; it tends to be designed as a Wi-Fi Hotspot. Every EN is associated with FN through a Wi-Fi interface. Every FN is assigned to a Class C IP (Internet protocol) Address Block, as "192.168.0.0" to "192.168.255.255", IP pools for interfacing ENs (EEi). These IPs can be assigned for every EN through the inbuilt DHCP server of FN from the above IP pools automatically.

As it very well can be worked with the "MQTT protocol", where FN is the server and EN is the client. Essential Routing software can enable the communication between Wi-Fi-to-Wi-Fi networks for the association of each FN to FNBS, referring to "Raspberry Pi documentation" [19] for limited distances. Where the Wi-Fi network is unimaginable there might be a "Long-distance communication protocol (LoRa)" specialized gadget connected through the GPIO port of the "Raspberry Pi" board. LoRa might be utilized as a standard connection point for long-distance communication, as the distance between FN and FNBS is significantly high. Otherwise, one more USB Wi-Fi dongle can be connected to FN to establish a wireless link between FNs to FNBS. A few FN gadgets can be made as a "Fog Node Cluster" group, in a geological area for correspondence at last to Cloudlet Server through FNBSs. A GPS peripheral transceiver can be associated with each FN so that the location information of the FN can be captured through the FN payload data. The location information can be set in the open-source map (e.g. Google map) for distinguishing the coordinate location of FNs. "NEO-6M GPS" can be selected as a GPS peripheral that can be interfaced through the UART port of the "Raspberry Pi" GPIO. It should likewise be associated with an RTC, fundamental for the blockchain Time stamp (7 Byte) through an I2C Bus interface, as in **Figure – 2**.

V.III. **FOG NODE BASE STATION (FNBS)**

The Fog Node Base Station (FNBS) is the topmost-level Node that is straightforwardly associated with the internet cloud through a built-in Ethernet Port. FNBSs are a "Raspberry Pi 4 with 8 GB" microcontroller board, but no sensors are associated with FNBS. This tiny Board can run with an open-source embedded Linux OS. The same can be downloaded from the "Raspberry Pi" site and installed as well. In our framework, we have utilized a 64-bit "Raspberry Pi" operating system, which is a "Debian Linux OS", which was referenced before in EN and FN. All FNs are associated with this FNBS through a "Long-distance communication protocol" (LoRa) port, where FNs are put at a significant distance from the FNBS. The same can also be connected through a separate Wi-Fi dongle of FN for a short distance. Every EN has a unique ID (2 Byte) of that WSN, and it frames as an "Edge Node Cluster" Group. Essentially, all FNs in a specific Geographical region likewise structure a "Fog Node Cluster" Group as above. Each Fog Node also has a separate unique ID (2 Byte) of that WSN. The data payloads of the EN carry and convey these unique IDs of both EN as well as FN. The EN isn't permitted to speak with more than one FN simultaneously. Likewise, the data payloads of the FN carry and convey this Unique ID of the FNBS, along with the Location information of FNs. Thus, FNs are not permitted to speak with more than one FNBS. The FNBSs are associated with the Cloudlet Server through the internet cloud, where all monitoring data information can be kept. The entire design of the whole architecture is shown above in, **Figure – 5**. Finally, MIS can be created for general surveillance, maintenance, well-being, usage of electric power, upkeep information, and so on.

V.IV **PROPOSED HYBRID BLOCKCHAIN MODEL**

Figure – 6, shows the essential Design of the proposed "Hybrid Blockchain Model". The FNs are associated with a public blockchain, whereas ENs are associated with a private blockchain. The associated public blockchain of FNs is an unauthenticated blockchain to submit transactions, and through network agreement, they can make a decentralized trust network. The public blockchain can't uphold the IoT's real-time needs on the off chance that all its FNs are added to it as incessant validation and authentication tasks would require a ton of assets and the equivalent is a tedious interaction. Since Nodes in different WSNs have a place with isolated administrators (FNBSs), they can't join the private blockchain utilizing a unified validation authentication process. Private blockchain Nodes (ENs) should be approved to join the network. A hybrid blockchain approach is demonstrated in, **Figure – 5**, to fit this network idea in this article. Two network concepts, private blockchain and public blockchain are combined in this hybrid blockchain model. Consequently, in this network, it tends to be the conceivable limit of 64k ENs with a solitary FN, associated through a private blockchain. Essentially, it very well may be conceivable to limit 64k quantities of FNs under a solitary FNBS, associated with a public blockchain. Thus, 64k quantities of FNBSs are likewise conceivable in the network. This multitude of nodes is feasible to interface through a Class C IP (internet protocol) address block, as referenced previously.

VI. **CONCLUSION**

The trading protocol and information-securing frameworks of each environmentally friendly generating unit are proposed briefly in this article. These units are under 1 kVA power (typically 720 VA). Total energy generation by each prosumer as well as total energy consumption by each prosumer and consumer, can be computed easily in a defined period, through this proposed system. It can also explain the surveillance, well-being, and maintenance information of the same units, along with their coordinate location (FNs). Finally, the same data can be placed for future MIS with GPS-enabled for the entire cluster of environmentally friendly generating units. A similar trading system can likewise be carried out not just in energy trading applications, it can likewise be executed in other comparative surveillance frameworks for instance the application in the Farming field and so on.

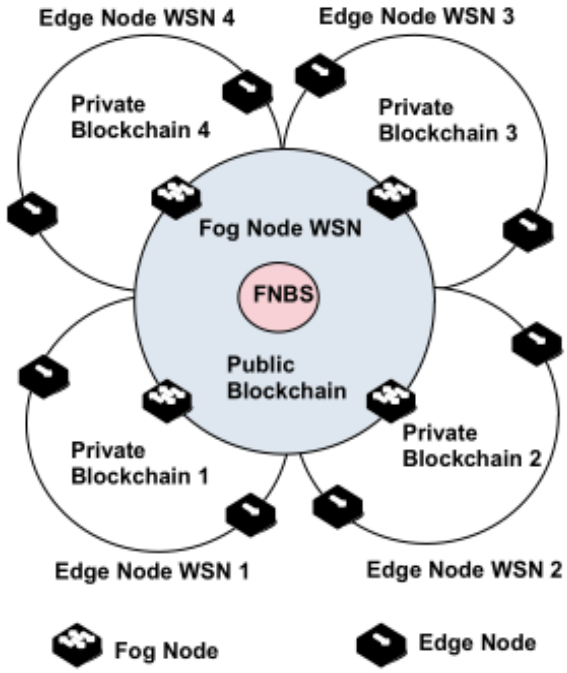

Figure – 6: The Basic Hybrid blockchain architecture

VII. REFERENCES

[1] S. Mishra, C. J. Crasta, C. Bordin, and J. Mateo-Fornés, "Smart contract formation enabling energy-as-a-service in a virtual power plant," *International Journal of Energy Research, published by, John Wiley & Sons Ltd*, vol. 46, no. 3, pp. 3272–3294, Oct. 2021, doi: 10.1002/er.7381.

[2] Z. Cui *et al.*, "A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN," *IEEE Trans Serv Comput*, vol. 13, no. 2, pp. 241–251, Mar. 2020, doi: 10.1109/TSC.2020.2964537.

[3] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication Protocols for Internet of Things: A Comprehensive Survey," *Security and Communication Networks*, vol. 2017. Hindawi Limited, pp. 1–41, 2017. doi: 10.1155/2017/6562953.

[4] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet Things J*, vol. 6, no. 3, pp. 4650–4659, Oct. 2019, doi: 10.1109/JIOT.2018.2874095.

[5] J. Huang, L. Kong, G. Chen, M. Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial iot: Blockchain system with credit-based consensus mechanism," *IEEE Trans Industr Inform*, vol. 15, no. 6, pp. 3680–3689, Mar. 2019, doi: 10.1109/TII.2019.2903342.

[6] M. J. A. Baig, M. T. Iqbal, M. Jamil, and J. Khan, "Design and implementation of an open-Source IoT and blockchain-based peer-to-peer energy trading platform using ESP32-S2, Node-Red and, MQTT protocol," *Energy Reports (Elsevier Ltd)*, vol. 7, pp. 5733–5746, Nov. 2021, doi: 10.1016/j.egyr.2021.08.190.

[7] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Comput Secur*, vol. 78, pp. 126–142, Jun. 2018, doi: 10.1016/j.cose.2018.06.004.

[8] Koirala N *et al.*, "Review of Low Head Turbines System of Nepal for Rural Electrification," in *6th IEEE International Conference on Renewable Energy Research and Application*, San Diego, USA: IEEE International Conference on Renewable Energy Research and Application, Nov. 2017, pp. 881–869.

[9] Rana Kailash and Meena Duli Chand, "Self Excited Induction Generator for Isolated Pico Hydro Station in Remote Areas," in *2nd IEEE International conference on power Electronics, Intelligent Control and Energy systems*, 2nd IEEE International conference on power Electronics, Intelligent Control and Energy systems, 2018, pp. 821–826.

[10] Xi-Tong Li, Hai-ju Kuang, and Litifu Zulati, "Planning of Renewable Energy Considering the Conditions of System Control and Location," in *IEEE International Conference on Advanced Mechatronic Systems, Luoyang, China, September 25-27, 2013*, Luoyang, China: IEEE Proceedings of the 2013, 2013, pp. 613–618.

[11] T. Adegbija, A. Rogacs, C. Patel, and A. Gordon-Ross, "Microprocessor optimizations for the internet of things: A survey," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 1, pp. 7–20, Jan. 2018, doi: 10.1109/TCAD.2017.2717782.

[12] S. Benedict, "Serverless Blockchain-Enabled Architecture for IoT Societal Applications," *IEEE Trans Comput Soc Syst*, vol. 7, no. 5, pp. 1146–1158, Oct. 2020, doi: 10.1109/TCSS.2020.3008995.

[13] K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, "Differential Privacy-Based Blockchain for Industrial Internet-of-Things," *IEEE Trans Industr Inform*, vol. 16, no. 6, pp. 4156–4165, Jun. 2019, doi: 10.1109/TII.2019.2948094.

[14] R. K. Kodali and S. R. Soratkal, "MQTT based home automation system using ESP8266," in *IEEE Region 10 Humanitarian Technology Conference 2016, R10-HTC 2016 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Apr. 2017. doi: 10.1109/R10-HTC.2016.7906845.

[15] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future

Challenges," *IEEE Access*, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp. 3343–3363, 2020. doi: 10.1109/ACCESS.2019.2962829.

[16] P. Zheng, Z. Zheng, X. Luo, X. Chen, and X. Liu, "A detailed and real-time performance monitoring framework for blockchain systems," in *ACM/IEEE 40th International Conference on Software Engineering: Software Engineering in Practice*, Gothenburg, Sweden: IEEE Computer Society, May 2018, pp. 134–143. doi: 10.1145/3183519.3183546.

[17] Z. Bao, W. Shi, D. He, and K.-K. R. Chood, "IoTChain: A Three-Tier Blockchain-based IoT Security Architecture," *ArXiv*, vol. v2, Jun. 2018, [Online]. Available: http://arxiv.org/abs/1806.02008

[18] P. P. Bhattacharjee, C. Koley, and S. Chatterjee, "Chapter 26, 'Blockchain-Based Clean and Green Energy (Pico Hydel Power) Monitoring System,'" in *Lecture Notes in Electrical Engineering, Advances in Communication, Devices and Networking, Proceedings of ICCDN 2022*, 1st ed., vol. 1037, S. Dhar, D.-T. Do, S. N. Sur, and C.-M. Liu, Eds., Rangpo, Sikkim, India: Springer Nature Science and Business Media LLC, 2023, pp. 253–269. doi: https://doi.org/10.1007/978-981-99-1983-3.

[19] Bradbury. Alex, "Raspberry Pi Documentation and Configuration (The raspi-config Tool)," Raspberry Pi Ltd. Accessed: Apr. 28, 2022. [Online]. Available: https://www.raspberrypi.com/documentation/computers/configuration.html